

**Anti-money Laundering, Combating the Financing of
Terrorism and Proliferation of Weapons of Mass
Destruction (AML/CFT/CFP) Policy**

CARRER N.V.

Dr. Henri Fergusonweg 1, Gaito, Willemstad, Curaçao

February 2025

Document Information

Subject	AML/CFT/CFP Policy
Purpose	Company procedures for Anti-Money Laundering, Fraud and Payments ongoing tasks
Involvements	All departments
Responsibility	MLRO
Approval	Director
Review	Annually or earlier as needed
Classification	Company Confidential
Version	2.0
Updated By	MLRO
Authorised By	Director
Distribution Date	27/02/2025

1. Introduction

“Money laundering” is generally defined as “engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds so that those proceeds appear to have been derived from legitimate activities or origins or otherwise constitute legitimate assets.”

“Terrorist Financing” is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act. The money involved in a terrorist financing act is not necessarily derived from illicit proceeds

“Financing of Proliferation of weapons of mass destruction” is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

The Proceeds of Crime are funds derived from illicit sources and from which a benefit or enjoyment may be obtained. Although the aim is not to launder the funds or to fund terrorism or proliferation, it is still considered to be an illegal activity and subject persons should be aware of such activity and must report it as if it was ML/FT//FP.

The policies set forth herein (the “Policies”) are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to Carrer N.V. (or the “Company”) in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism.

The Company is aware that criminals and terrorists may attempt to use the Company’s services to channel funds from illegal activities.

2. Scope of the Policy

The scope of this policy is to establish Policies from which procedures on internal control, risk assessment, risk management and compliance in relation to AML/CFT/CFP will be drawn up.

Users of this and related policies should also refer, where relevant, to the Applicable Laws and any other relevant measures/guidelines which may be issued from time to time by the Financial Action Task Force ("FATF") and/or any relevant authority or agency.

Unless the context requires otherwise, words and expressions used in the Policies shall have the same meaning as that set out in the applicable laws and regulations.

The Company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to ML/FT/FP.

The Company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent ML/FT/FP and to ensure any suspicious activities are escalated to the relevant authorities.

The Policies outline the general and minimum standards of internal anti-money laundering, combating the financing of terrorism and the financing of proliferation of weapons of mass destruction (AML/CFT/CFP) Policies which should be adhered to by the Company's management and employees.

3. Money Laundering Reporting Officer (MLRO)

Within the Company's internal control framework, there key role for AML/CFT/CFP compliance - the Money Laundering Reporting Officer (MLRO). MLRO responsibilities shall include but are not limited to:

- Develop and update internal policies and procedures on AML/CFT/CFP.
- Monitor and test the effectiveness of these procedures on an ongoing basis.
- Prepare and submit annual AML/CFT/CFP compliance reports to senior management.
- Analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions.
- Review all internally reported unusual transactions for their completeness and accuracy against other sources.
- Keep records of internally and externally reported unusual transactions.
- Design an internal procedure specifying when the reporting of unusual transactions will lead to blocking/freezing of user accounts, taking into account the risk of tipping off the player, and conduct closer investigations of unusual transactions if necessary.
- Prepare external reports of unusual transactions, receiving and evaluating all internal Suspicious Transaction Reports (STRs).
- Liaise with the Financial Intelligence Unit (FIU) and law enforcement agencies.
- Decide whether to file external Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR).
- Design, implement and update the AML program.
- Ensure customer due diligence measures and ongoing monitoring.
- Maintain records, including those related to internally and externally reported unusual transactions.
- Execute internal control procedures.
- Perform internal auditing of AML/CFT/CFP processes (unless a dedicated internal auditing function is available).
- Monitor and manage compliance with, and the internal communication of, such policies and procedures.
- Monitor relevant staff and agent screening processes.
- Conduct self-education and ensure the education of relevant staff in AML/CFT/CFP on an annual basis, or more regularly if deemed necessary.
- Organize training sessions for staff on various compliance-related issues.
- Remain informed on local and international developments in AML/CFT/CFP and make suggestions to management for improvements.

- Prepare periodic reports on the casino's efforts against money laundering, financing of terrorism, and financing of proliferation.
- Liaise with law enforcement authorities.
- Manage Investigation Order requests received from the authorities.

A Money Laundering Reporting Officer (MLRO) is appointed to be the business owner of AML/CFT/CFP Risk Assessment, Controls, Policies and Procedures. The MLRO appointed should possess professional experience, training and resources to carry out his/her appointment as per Applicable Laws.

4. Risk Assessment

4.1. Business ML/TF/PF Risk

The Company is to carry out a yearly risk assessment to identify the ML/TF/PF risks the Company is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risk. The Business Risk Assessment will identify the following risks:

- identify ML/TF/PF Vulnerabilities;
- identify ML/TF/PF Threats; and
- identify any new requirements.

Based on the results of the Business ML/TF/PF Risk Assessment and if deemed necessary, in order to minimize any new risks identified or existing risks being re-classified, the following controls would need to be revisited and amended accordingly:

- measures;
- policies;
- controls; and
- procedures.

The Business ML/TF/PF Risk Assessment should be monitored and improved whenever substantial changes to the Company's systems, processes, new markets, new games, regulatory changes and overall operations.

The Business ML/TF/PF Risk Assessment and related measures, policies, controls and procedures are to be recorded and made readily available for review by the interested authorities at any time.

4.2. Customer ML/TF/PF Risk

As each customer exposes the Company to different risks, a player-specific risk assessment must be carried out so the Company is able to identify the potential risks it faces when entering into a business relationship with, or carrying out an occasional transaction for a player. The customers risk assessment is based on:

- customer type;
- products used (e.g. sportsbook);
- services (e.g. poker, bingo);
- transactions/payment systems;
- delivery channels; and
- geographical origin of the customer and/or payment method.

The assessment enables the Company to develop a risk profile for the customer and to categorize the ML/TF/PF risk posed by such player/customer as low, medium or high.

After registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to reconsider risk level depending on changes in customer's

activity and to establish the point of reaching the relevant due diligence requirements thresholds.

5. Sanctions and PEP Status Screening

All players are screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the Company also takes that local list into account. The Company does not do business with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a player, the Company checks published lists of known or suspected terrorists or other sanctioned persons or companies:

- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists | Office of Foreign Assets Control (treasury.gov);
- EU Sanctions List <http://www.sanctionsmap.eu/#/main>.

Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the Company regularly screens for PEP status during the business relationship.

6. Customer Due Diligence

Customer Due Diligence (CDD) Measures include:

- collection of identification details;
- verifying the identity of the customer;
- determining the customer profile and levels of activity and adjusting the profile as and when necessary;
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the results of the risk assessment; and
- retention of records of these checks and update them when there are changes.

The CDD Procedure defines the procedure used to carry out CDD including timeframes when this will be triggered and in which cases Enhanced Due Diligence will need to be performed.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their account restricted during this period.

Should the CDD Procedure not be completed within the established timeframes of such a request, the customer's account will be considered to have failed completing CDD and thus will be denied from any further activity. The raising of a Suspicious Transaction Report (STR) is to be considered. Such a decision is to be taken and recorded by the MLRO.

Unless a STR has been raised and an appropriate period has passed in which the customer has still not completed CDD, the account may be closed, and deposited funds still present on the customer's account will be returned to the deposit method, where possible, less any charges incurred by the business for transmission to this destination.

7. Payment Methods

The Company will not accept to receive or make cash deposits or payments in relation to customer's activities.

The Company will only make use of payment methods that are:

- offered by licensed financial institutions and regulated by financial regulator; and
- if integrated through payment service providers, these would have been approved.

The Company will hold received payments from customers into a player's account, distinct from Company accounts.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers, together with any transfers of funds that are made into or out of the player's account for settling the customer's remote gaming activity. It will also be able to identify when thresholds for CDD have been reached.

In all instances, where possible, funds returned to customers shall be returned to the customer's originating payment method. If this is not possible due to the nature of the payment method or in case of the account not being available any more to receive funds, payments will be transferred only to the bank account in the customer's name, following the completion of the CDD process.

8. Suspicious Transaction Report

An internal Suspicious Transaction Report is to be sent directly to the MLRO whenever there is a suspicion that a customer is engaged in ML/TF/PF.

No one is to divulge to co-workers, line managers and especially the customer/s that an STR has been raised as this is potentially considered to be 'tipping-off'. An employee who raises an STR must escalate directly to the MLRO.

9. Notifications of Fraud and Law Enforcement or Regulatory Authorities' requests

The Company will record and take appropriate actions whenever a notification of fraud or requests by Law Enforcement or relevant Regulatory Authorities are received. The Company will follow a due process to ensure such notifications or requests are processed without delay and the Company will, within its abilities, to assist such authorities effectively.

Law Enforcement and Regulatory authorities' notifications may also provide just cause to ensure the Company's Responsible Gambling, Fraud, Money Laundering and Terrorist Funding risk mitigation strategies are working effectively. Where gaps are identified, the Company will take immediate action to resolve such gaps.

10. Employee Training

Within an appropriate period of the commencement of employment, employees are to be provided with ML/FT/FP training to ensure they are aware of measures, policies, controls and procedures that are in force. This training shall include:

- general awareness of Money Laundering / Terrorism Funding for all employees;
- specific Guidance on the related measures, controls, policies and procedures in place within the Company for employees specifically occupying roles related to AML/CFT/CFP Controls and Compliance;
- an assessment to ensure that the employee has grasped the key points of training received.

The training provided to employees is to be recorded and refreshed at least annually. Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the Company's Policies against money laundering and terrorist financing. Training process and its contents differs from the type of employees to be trained: new employees, audit staff, AML compliance staff, supervisors and managers, senior management and board of directors and etc. and is conducted in accordance with applicable laws and regulations.

The MLRO is also required to attend annual refresher training and to keep up to date with the subject.

In order to be able to demonstrate that it has complied with the guidelines with respect to training, the Company will maintain records which include:

- details of the content of the training programs provided;
- the names of the person(s) who have received the training;
- the date on which the training was provided;
- the results of any testing carried out to measure the participants' understanding of the AML/CFT/CFP requirements; and
- an ongoing training plan.

Further information about employee training may be found in the Human Resources' relevant policies and procedures.

11. Employee Screening

The Company's prospective employees that are to be involved with or connected to activities that would fall within the scope of this Policies, are to be screened before they are employed. The Company is to ensure that they are fit and proper to occupy positions in which they will participate in the provision of services to the customer. Third party screening providers may be engaged to ensure this.

The Company will carry out monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the Company's operations and obligations. The Company will at all times do its utmost to respect the privacy of its employees.

Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO and / or Director directly and should they wish to remain anonymous, to do this via an anonymous letter or e-mail service providing as much facts and information as possible.

12. Retention of Records

Company will maintain, for at least five years, all necessary records on transactions to enable them to comply with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Such records may include:

- all registration details;
- identification verification details;
- standard and enhanced due diligence items;
- suspended accounts and reason for suspension;
- closed accounts;
- financial transactions – deposits, bets made, withdrawals, prize payments;
- self-exclusion periods (temporary and permanent);
- self-imposed limits;
- excluded players;
- complaints and responses;
- audit trails;
- bank reconciliations;
- Customer Service electronic correspondence records.

All records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

End of the customer relationship is defined as from the last day the customer effected any movement of funds to and from their account, or a successful login.

Should statutory obligations arising from other laws, regulations or based on a request from a regulator, a requirement be established to keep records for a longer period be in place, this will be taken in consideration and adhered to.

Documents will not be retained beyond the required obligations and will be deleted.

Approved by
Vivian Ersilia, o.b.o. (SMES)
Solutions for Management and
Employment Support N.V. as
Managing director



Date: 23.04.2025

Annex No.1 | References

Applicable Laws means the following:

National regulations:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);
- National Ordinance on the Obligation to report Cross-border Money Transportation (N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

International regulations:

- Caribbean Financial Action Task Force regulations www.cfatf-gafic.org.
- FATF regulations – www.fatf-gafi.org – High-risk and other monitored jurisdictions (published on FATF Website and updated regularly).
- United Nations - Financial Sanctions Consolidated List.
- European Union – Consolidated list of sanctions, AML/CFT/CFP Information page.

Approved by
Vivian Ersilia, o.b.o. (SMES)
Solutions for Management and
Employment Support N.V. as
Managing director



Date: 23.04.2025

Annex No. 2 | Glossary of Terms

- AML – Anti-Money Laundering
- CDD – Customer Due Diligence
- CFT – Combatting the Financing of Terrorism
- CFP – Combating the Financing of Proliferation of weapons of mass destruction
- EDD – Enhanced Due Diligence
- DE – Designated Employee
- FATF – Financial Action Task Force (www.fatf-gafi.org)
- MLRO – Money Laundering Reporting Officer
- PEP – Politically Exposed Persons
- RBA – Risk Based Approach
- SAR – Suspicious Activity Report
- SDD – Simplified Due Diligence
- STR – Suspicious Transaction Report

Approved by
Vivian Ersilia, o.b.o. (SMES)
Solutions for Management and
Employment Support N.V. as
Managing director



Date: 23.04.2025